

Cyclic codes

6th January 2005

Definition 1. A subset S of $\mathbf{F}_q^n$ is *cyclic* if $(a_0, \dots, a_{n-1}) \in S$ implies $(a_{n-1}, a_0, \dots, a_{n-2}) \in S$. A linear code C is called a *cyclic code* if C is a cyclic set. The word

$$(u_{n-r}, \dots, u_{n-1}, u_0, u_1, \dots, u_{n-r-1})$$

is said to be obtained from the word $(u_0, \dots, u_{n-1})$ in $\mathbf{F}_q^n$ by cyclically shifting r positions. §

Definition 2. Let R be a ring. A nonempty subset I of R is called an *ideal* if both $a + b$ and $a - b$ belong to I and $r \cdot a$ is in I , for all a and b in I and r in R . §

Note 1. $\mathbf{F}_q^n$, also denoted by $V(n, q)$, is the vector space of all vectors of length n over $\mathbf{F}_q$, which is also known as $GF(q)$. Here we suppose that n and q are relative primes of each other, that is to say, $(n, q) = 1$. §

Cyclic codes can also be defined as Definition 3.

Definition 3. Let θ be a mapping such that

$$\theta : \mathbf{F}_q^n \mapsto \mathbf{F}[x] / (x^n - 1)$$

where $(x^n - 1)$, sometimes denoted by $\langle x^n - 1 \rangle$, denotes the ideal of the polynomial ring $\mathbf{F}[x]$ generated by $x^n - 1$ by

$$\theta(a_0, \dots, a_{n-1}) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + \langle x^n - 1 \rangle$$

for all a_i in $\mathbf{F}_q$, $0 \leq i \leq n - 1$. In other words,

$$\theta : (a_0, \dots, a_{n-1}) \mapsto a_0 + a_1x + \dots + a_{n-1}x^{n-1}$$

§

Note 2. $\mathbf{F}[x] / (x^n - 1)$ is also a vector space over $\mathbf{F}$ is an $\mathbf{F}_q$ -linear transformation of vector spaces over $\mathbf{F}_q$. In fact it is a vector space isomorphism. We could identify $\mathbf{F}_q^n$ with $\mathbf{F}_q[x] / (x^n - 1)$, and a vector $\mathbf{u} = (a_0, \dots, a_{n-1})$ with the polynomial $a(x) = \sum_{i=0}^{n-1} a_i x^i$ §

Theorem 1. Let θ be the mapping defined in Definition 3, and let C be a linear code of length n over $\mathbf{F}_q$. Then C is a cyclic code if and only if $\theta(C)$ is an ideal in the quotient ring $\mathbf{F}[x] / (x^n - 1)$.

Proof. Since C is a linear code of length n over $\mathbf{F}_q$, it is a subspace of the vector space $\mathbf{F}_q^n$, and $\theta(C)$ a subspace of $\mathbf{F}[x] / (x^n - 1)$. Let $(a_0, \dots, a_{n-1})$ be in C . Then $(a_{n-1}, a_0, \dots, a_{n-2})$ is in C if and only if

$$a_{n-1} + a_0x + \dots + a_{n-2}x^{n-1} + \langle x^n - 1 \rangle = x(a_0 + a_1x + \dots + a_{n-1}x^{n-1}) + \langle x^n - 1 \rangle$$

is in $\theta(C)$. ¶

Example 1. Recall that a $[n, k, d]$ -linear code is a code of distance d , length n and the number of elements in the bases k . Then the binary $[3, 2, 2]$ -linear code $\{000, 110, 101, 011\}$ is a cyclic code and $\theta(C) = \{0, 1 + x, 1 + x^2, x + x^2\}$ is a subset of $\mathbf{F}_2[x] / (x^3 - 1)$. Moreover, $\theta(C)$ is an ideal.

Example 2. The set of all the integers divisible by a fixed positive integer m is an ideal of $\mathbf{Z}$. All the polynomials in the polynomial ring $\mathbf{F}_q[x]$ that are divisible by a fixed, non-zero polynomial $f(x)$ form an ideal.

Definition 4. An ideal I of a ring R is called a *principal ideal* if there exists an element g in I such that

$$I = \langle g \rangle = \{gr : r \in R\}$$

The element g is called a *generator* of I , and I is said to be generated by g . A ring is called a *principal ideal ring* if all its ideals are principal.

§

Bibliography

Raymond Hill. *A first course in coding theory*. Clarendon, 1986

San Ling and Chaoping Xing. *Coding theory, a first course*. Cambridge University Press, 2004

L R Verma. *Elements of algebraic coding theory*. Chapman & Hall, 1996